REMARKS/ARGUMENTS

This paper is being provided in response to the Office Action dated November 13, 2007 for the above-referenced application. In this response, Applicant has canceled Claims 2, 23, and 42, and amended Claims 1, 3-5, 22, 24-26, 41, and 43-45. Applicant respectfully submits that the claim amendments are supported by the originally filed application.

The rejection of Claims 1-7, 22-28, 41-52, 63-66, and 71 under 35 U.S.C. § 103(a) as being unpatentable over Waldin et al (U.S. Patent No. 6,094,731 hereinafter referred to as "Waldin") in view of Drew (U.S. Patent No. 6,928,555, hereinafter "Drew") is hereby traversed and reconsideration thereof is respectfully requested. This rejection as applied to Claims 2, 23 and 42 is moot in view of the cancellation of these claims herein.

Claim 1, as amended herein, recites a computer implemented method of scanning a storage device for viruses, comprising: determining, by the storage device, each track of the storage device that has been accessed for a write operation since a previous virus scan using information about tracks of the storage device without using information about a file structure, a file system, or a file type; providing, to an antivirus unit by the storage device, information indicating which tracks of the storage device have been accessed for a write operation since the previous virus scan; and scanning, by the antivirus unit using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous virus scan for viruses, wherein scanning is performed without using information about a file structure, file system or a file type. Claims 3-7, 63 and 66 depend from Claim 1.

Claim 22, as amended herein, recites a computer program product for scanning a storage device for viruses, the computer program product including a computer-readable medium with executable code stored thereon for: determining, by the storage device, each track of the storage device that has been accessed for a write operation since a previous virus scan using information about tracks of the storage device without using information about a file structure, a file system, or a file type; providing, to an antivirus unit by the storage device, information indicating which tracks of the storage device have been accessed for a write operation since the previous virus scan; and scanning, by the antivirus unit using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous virus scan for viruses, wherein scanning is performed without using information about a file structure, a file system, or a file type Claims 23-28, and 64 depend from Claim 22.

Claim 41, as amended herein, recites an antivirus unit, comprising: means for coupling to at least one storage device; means for determining each track of the storage device that has been accessed for a write operation since a previous virus scan using information about tracks of the storage device without using information about a file structure, a file system, or a file type; means for receiving, from the at least one storage device, information determined by the at least one storage device indicating which tracks of the at least one storage device have been accessed for a write operation since the previous virus scan; and means for scanning, using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous virus scan for viruses, wherein scanning is performed without using information about a file structure, a file system, or a file type. Claims 43-52, 65 and 71 depend from Claim 41.

Waldin discloses a system, method and computer readable medium for examining a file associated with an originating computer to determine whether a virus is present within the file. (See Abstract). Waldin discloses scanning a file and placing into a critical sectors file the identification (e.g., number) of each sector that is scanned. As each sector is operated upon, a hash value is calculated for that sector and inserted into the critical sectors file along with the size of the file scanned. (Col. 4, Lines 52-64; Figures 1 and 2). Waldin's Figure 1 includes antivirus modules on an originating computer 2 and a recipient computer 11 and processing performed on each of the computer systems when transmitting a file from an originating computer to a recipient computer. (See Figure 1; Col. 3, Lines 22-34). Waldin's Figure 3 determines if computed hash values for file 1 match stored hash values for file 1. If not, the entire file 1 is rescanned. (Steps 36, 37 of Figure 3; Col. 6, Lines 43-46; See also Col. 2, Lines 24-26). Waldin discloses determining hash values for only those sectors of a file actually retrieved by module 5 of Figure 1. Module 3 of Waldin's Figure 1 always scans the same set of sectors of a file unless the file changes in length or the contents of those sectors changes in some way. The antivirus accelerator module 5 automatically hashes all sectors scanned by module 3 in the same way regardless of contents of the sectors. No new parser of hasher coding needs to be performed and incorporated into module 5 to support new file formats. (Col. 7, Line 35-Col. 8, Line 2).

Drew is cited on pages 4-5 of the Office Action as support for disclosing detecting, by a storage device, write operations to tracks of the storage device; providing to an antivirus unit by the storage device information indicating which tracks of the storage device have been accessed for a write operation; and scanning portions on those tracks to which write operations have been directed in accordance with information provided by the storage device (Col. 3, Lines 40-55; Col. 4, Lines 5-25).

Col. 3, Lines 40-55 of Drew refer to steps of the flowchart of Drew's Figure 2 with respect to processing performed with reference to Figure 1 in which an antivirus program is included in the network server computer 4. After opening a file for write access (step 22), the file is scanned for viruses (step 24). If no viruses are detected, the file is provided to the application program (step 26). A period of time after the file is opened, a file closure request is made (step 28). Upon the file closure request being made, the typical antivirus program loaded into a computer system, such as network server computer 4, interfaces with the network operating system to scan the file for viruses.

Col. 4, Lines 5-25 of Drew make reference to Drew's Figure 3 which includes the steps of Figure 2 with new steps 40 and 42. Step 40 determines whether a file was actually written, that is modified by the user performing some writing step on the open file. This latter citation of Drew discloses use of a modification flag set by the operating system. The computer coding for step 40 determines whether an open file was actually written or modified by looking for a flag in the operating system indicative of such a modification.

Claim 1, as amended herein, is neither disclosed nor suggested by the references, separately or in combination, in that the references do not disclose or suggest at least the features of ***a computer implemented method of scanning a storage device for viruses, comprising: determining, by the storage device, each track of the storage device that has been accessed for a write operation since a previous virus scan using information about tracks of the storage***

device without using information about a file structure, a file system, or a file type; providing, to an antivirus unit by the storage device, information indicating which tracks of the storage device have been accessed for a write operation since the previous virus scan; and scanning, by the antivirus unit using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous virus scan for viruses, wherein scanning is performed without using information about a file structure, file system or a file type, as set forth in Claim 1.

Regarding the first recited step of amended Claim 1, the references do not disclose or suggest ***determining, by the storage device, each track of the storage device that has been accessed for a write operation since a previous virus scan using information about tracks of the storage device without using information about a file structure, a file system, or a file type.*** Waldin discloses comparing hash values for sectors of a file to determine if there have been changes to the file. However, Waldin makes no mention of operating on tracks of a storage device. Regarding Drew, as pointed out above, Drew discloses determining whether an open file was actually written, that is, modified by the user performing some writing step on the open file. Drew discloses determining whether a file that has been opened was written to or modified. Drew does not disclose or suggest determining each track of the storage device that has been accessed for a write operation since a previous scan.

Furthermore, for purposes of argument only, even if Drew's disclosure of determining files that have been modified suggests determining each track of the storage device accessed for a write operation since a previous scan, the references make no disclosure or suggestion of the storage device performing the determining step, and the references do not disclose or suggest making such a determination without using information about a file structure, file system or file type. The references, and in particular Drew, make no mention of the storage device performing the first determining step. In distinct contrast, Drew discloses use of a modification flag set by the operating system of the server computer. For reasons set forth in Applicant's previous amendment and response, Waldin does not disclose or suggest making such a determination without using information about a file structure, file system or file type. Regarding Drew, Drew also uses information about the file, such as information about a file structure, file system or file type. Setting a flag on a per file basis as to whether the file has been written or modified, as in Drew, does not disclose or suggest determining each track of the storage device accessed for a write operation since a previous scan using information about tracks of the storage device without using information about a file structure, a file system, or a file type, as recited in Claim 1.

Regarding the second recited step of amended Claim 1, the references do not disclose or suggest ***providing, to an antivirus unit by the storage device, information indicating which tracks of the storage device have been accessed for a write operation since the previous virus scan.*** Waldin is silent regarding the foregoing providing step since, as pointed out above, Waldin makes no disclosure or suggestion of determining such information about each track and thus, cannot provide any such information to an antivirus unit. Based on Applicant's reading of Drew, Drew discloses an anti-virus program loaded into the server computer 4 and the server computer determining when a file has been modified using information of the server computer. There is no disclosure or suggestion in Drew of the server computer, or the anti-virus program thereon, receiving any information from a storage device indicating which tracks of the storage device have been accessed for a write operation. Rather, Drew's disclosure indicates that the server computer does not receive information regarding file modifications from a storage device since the modification flag is set by the operating system. Thus, there appears to be no reason for the storage device to provide any information regarding write operations to the antivirus program on the computer 4 since such information is already available on the server 4 where the antivirus program resides.

Regarding the third recited step of Claim 1, the references do not disclose or suggest ***scanning, by the antivirus unit using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous virus scan for viruses, wherein scanning is performed without using information about a file structure, file system or a file type.*** Waldin is silent regarding the foregoing step for at least the reasons pointed out above that Waldin makes no disclosure or suggestion of the recited information indicating which tracks of the storage device have been accessed for a write operation since the previous virus scan. Drew discloses scanning previously opened files that have been written to. Drew does not disclose performing scanning with respect to each track identified as having been accessed for a write operation.

Furthermore, for purposes of argument only, even if Drew's disclosure of scanning previously opened files that have been modified as indicated by a modification flag somehow suggests scanning at least a portion of each track determined as having been accessed for a write operation since a previous scan, Drew makes no disclosure or suggestion of performing scanning using the information (the same "information" as recited in the previous providing step) provided by the storage device. Drew's scanning also makes use of information about files and thus does not perform scanning without using information about a file structure, file system or a file type as recited in Claim 1.

Applicant notes that when a file is scanned, those portions of the storage device associated with the file are scanned. In order for Drew and Waldin to perform the scanning, information about the file, such as information about file structure, file system or a file type, is used in order to determine, among other things, where the file is located on the storage device. Without such information, Applicant respectfully submits that the scanning as performed in Drew as well as Waldin cannot be performed. In contrast, Applicant's Claim 1 recites that scanning is performed without using information about a file structure, file system or a file type.

In connection with the Response to Arguments set forth in Pages 2-3 of the Office Action, as pointed out above, when a file is scanned, those portions of the storage device associated with the file are scanned. Furthermore, when performing scanning on files as disclosed in Drew, information about the files is used. When scanning a track, the entity being scanned pertains to a track and those portions of the storage device associated with the track. With respect to the scanning step of Claim 1, the portion scanned is included in one of the tracks identified as having been accessed for a write operation since the previous scan. Furthermore, as also recited in Claim 1, scanning is performed without using information about a file structure, file system or file type. Drew's disclosure of using information stored on a per file basis as to whether the file has been written or modified and then scanning the file if it has been modified does not disclose or suggest, as set forth in Claim 1, scanning, by the antivirus unit using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous virus scan for viruses, wherein scanning is performed without using information about a file structure, file system or a file type.

For at least the foregoing reasons, Applicant respectfully submits that the references do not disclose or fairly suggest the foregoing recited features of Claim 1. Claims that depend from Claim 1 are also neither disclosed nor suggested by the references for at least the same reasons as those set forth regarding Claim 1.

Applicant's independent Claims 22 and 41 recite features similar to those set forth above regarding Claim 1 that are neither disclosed nor suggested by the references. Thus, for reasons similar to those set forth above, Applicant's Claims 22 and 41, and claims that depend therefrom, are also neither disclosed nor suggested by the references.

Claims that depend from each of the independent Claims 1, 21, and 41 are not disclosed or suggested by the references for at least those reasons set forth above in connection with the independent claims. However, features set forth in the dependent claims are also neither disclosed nor suggested by the references.

In connection with Applicant's dependent Claim 52, page 6 of the Office Action cites to Col. 3, Lines 47-55 of Waldin as support for disclosing the recited features. Dependent Claim 52 recites, in part, ***wherein at least a portion of the antivirus unit is provided on at least some controllers for the at least one storage device***. Col. 3, Lines 47-55 of Waldin refer to Figure 1 including an originating computer 2 including modules 3, 5 and 12. Waldin discloses that file 1 included in RAM 10 could have originally been on a hard disk, floppy disk or any other computer readable medium, and could be brought into RAM 10 before being acted upon by modules 3, 5, and 12. Nowhere in this citation, or elsewhere Waldin, is there any disclosure or suggestion of including any portion of modules 3, 5, and 12 on a controller or other component of a storage device. Waldin's Figure 1 shows these modules as being included in the originating computer 2. Applicant respectfully submits that Drew also appears silent regarding any disclosure or suggestion of the features recited in Claim 52. As such, the references neither disclose nor suggest the features recited in dependent Claim 52.

In view of the foregoing, Applicant respectfully requests that the rejection be reconsidered and withdrawn.

The rejection of Claims 67-70 under 35 U.S.C. 103(a) as being unpatentable over Waldin and Drew and further in view of Ruff (U.S. Patent No. 6,802,028, hereinafter "Ruff"), is hereby traversed and reconsideration thereof is respectfully requested.

Claims 66-70 depend from independent Claim 1. Claim 1, and claims that depend therefrom, are neither disclosed nor suggested by Waldin and Drew for reasons set forth above. For reasons pointed out below, further combining Waldin and Drew with Ruff also does not disclose or suggest Claim 1, and claims that depend therefrom.

Ruff is cited on pages 6-7 of the Office Action as support for teaching an antivirus unit included in a disk controller of a storage device, wherein the disk controller is a first disk controller of a plurality of disk controllers included in the storage device, the antivirus unit is a first antivirus unit of a plurality of antivirus units included in the storage device and each of said plurality of disk controllers includes a different one of said plurality of antivirus units (Col. 7, Lin 53-Col. 8, Line 34).

Features of Claim 1 which are neither disclosed nor suggested by Waldin and Drew, taken separately or in combination, are pointed out above. Ruff also appears silent regarding any disclosure or suggestion of the foregoing recited features of Claim 1. Thus, combining Waldin and Drew with Ruff does not overcome the deficiencies of Waldin and Drew with respect to at least the foregoing features of Claim 1.

Claims 66-70 which depend from Claim 1 are neither disclosed nor suggested by the references for at least the same reasons as Claim 1. However, Applicant will point out some particular features of the dependent claims which are also neither disclosed nor suggested by the references.

Applicant's Claim 67 recites, in relevant part, ***wherein the antivirus unit is included in a disk controller of the storage device.*** Claim 68 also recites, in relevant part, ***wherein the antivirus unit is included as software running on the disk controller.*** As support for disclosing features of Claims 67 and 68, pages 6-7 of the Office Action rely on Ruff, Col. 7, Line 53-Col. 8, Line 34. The foregoing citation refers to Ruff's Figure 3 which includes a virus detector 312 in a computer system 100. The detector 312 is separate from the controller 306. Applicant cannot locate where in Figure 3, or in the foregoing citation of Ruff, is there disclosure or suggestion of the foregoing features of Claims 67 and 68. In contrast, Ruff's Figure 3 illustrates the virus detector as part of the computer system but not included in the controller.

In view of the foregoing, Applicant respectfully requests that the rejection be reconsidered and withdrawn.

Based on the above, Applicant respectfully requests that the Examiner reconsider and withdraw all outstanding rejections and objections. Favorable consideration and allowance are earnestly solicited. Should there be any questions after reviewing this paper, the Examiner is invited to contact the undersigned at 508-898-8604.

Respectfully submitted,
MUIRHEAD AND SATURNELLI, LLC

Anne E. Saturnelli
Registration No. 41,290

MUIRHEAD AND SATURNELLI, LLC
200 Friberg Parkway, Suite 1001
Westborough, MA 01581
Tel: (508) 898-8604
Fax: (508) 898-8602

Date: February 12, 2008